IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

APPEAL NO:

In Re Application of: Paul A. CRONCE et al.

Confirmation No.: 1789

Serial No.: 10/072,597

Filed: February 5, 2002

For: METHOD AND SYSTEM FOR DELIVERY OF SECURE SOFTWARE LICENSE INFORMATION

APPEAL BRIEF

Stephen G. Sullivan
Attorney for Appellants
Strategic Patent Group, P.C.
P.O. Box 1329
Mountain View, CA 94042

TOPICAL INDEX

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In Re Application of:	Date: September 17, 2007
Paul A. CRONCE	Confirmation No.: 1789
Serial No.: 10/072,597	Group Art Unit: 3621
Filed: February 5, 2002	Examiner: Bayat, Bradley B.

For: METHOD AND SYSTEM FOR DELIVERY OF SECURE SOFTWARE LICENSE INFORMATION

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Sir:

Appellant herein files an Appeal Brief drafted in accordance with the provisions of 37 C.F.R. §41.37 as follows:

I REAL PARTY IN INTEREST

Appellant respectfully submits that the above-captioned application is assigned, in its entirety to Pace Anti-Piracy of San Jose, CA.

II RELATED APPEALS AND INTERFERENCES

Co-pending application number 10/080,639, entitled "Delivery Of A Secure Software License For A Software Product And A Toolset For Creating The Software Product" filed on February 21, 2002, and assigned to the assignee of the present invention is also currently under appeal.

III STATUS OF CLAIMS

Application Serial No. 10/072,597 (the instant application), as originally filed, included claims 1-26. Claims 1-26 are presently pending. In response to the Office Action dated June 29, 2005, Claims 1, 11, 12, 15, 16, 23 and 24 were amended. In response to the Final Office Action dated January 23, 2006, claims 16 and 24 were amended. Claims 1-26 are on appeal and all applied prospective rejections concerning Claims 1-26 are being appealed herein.

IV STATUS OF AMENDMENTS

The Amendment under Rule 1.116 dated April 24, 2006, submitted in response to the Final Office Action dated January 23, 2006, was not entered by the Examiner (Notice of Abandonment 8/11/2006).

V SUMMARY OF CLAIMED SUBJECT MATTER

Independent claim 1 recites a method for the delivery of secure software license information to authorize use of a software product. Step (a) recites associating with a software publisher (page 13, line 19; page 14, line 4; page 15, line 13; and page 16, line 17) a private and public key pair (see software publisher's s digital certificate 502 page 13, line 19; and discussion of digital certificates in general, page 10 line 16+), wherein the software publisher provides the software product (page 5, line 16; page 6, line 23; page 7, line 7-9, 12, 16-17, 20, 22; page 8, line 23; page 9, line 16; page 10, line 2, 4, 6, 8; page 13, line 17, 20; page 14, line 2; page 15, line 2; page 16, line 16; page 21, line 4, 6, 13, 21-22; page 24, line 7, 11, 18-20; page 25, line 6, 11, 15, 19; and page 26, line 7, 19) and includes a software program (page 14, line 20; and page 24, line 4) and an authorization program (page 7, line 9, 12, 16-17, 24; page 9, line 24; page 13, line 13, 16, 18; page 14, line 11; page 16, line 5; page 17, line 21; page 23, line 21; page 24, line 21; page 25, line 11; and page 26, line 6, 8, 15, 18) within the software product (Specification, page 13, line 19; page 10 line 16 through page 12, line 13; and page 7, line 7-20, for example). Step (b) recites associating a product private key and public key with the software product, wherein at least one of the product private and public keys is digitally signed by the publisher private key, and including the product private and public keys with the authorization program (Specification, page 13, line 13-24, for example).

Step (c) recites upon invocation of the software product on a computer, (i) generating by the authorization program a license request (page 8, line 2-3, 6, 11, 16-17, 19, 22; page 9, line 2-3, 7, 13; page 10, line 14; page 14, line 15; page 15, line 7, 10; page 15, line 1, 11; page 16, line 2, 20; page 17, line 2-3, 7, 14-15, 20; page 19,

line 8; page 20, line 8-9, 11, 15, 19; page 21, line 2-3, 6, 10; page 22, line 1, 4-5, 14, 21-22; page 23, line 3; and page 24, line 8) containing user and product information, (ii) digitally signing the license request with the product private key, and (iii) transferring the signed license request to a key authority (Specification page 8, lines 2-3; page 14, line 10 through page 17, line 19; and page 8, lines 11-21, for example).

Step (d) recites in response to the key authority receiving the signed license request, (i) generating a license using data extracted from the license request and license terms, (ii) signing the license with the publisher private key, and (iii) transmitting the signed license to the authorizing program (Specification page 8, line 22 through page 9, line 22; page 22, line 1-22, for example). Step (e) recites validating the signed license using the publisher public key, and using the license terms to control the use of the software product (Specification page 9, line 23 through page 10 line 10; page 24, line 20 through page 25, line 17, for example).

Independent claim 12 is similar to claim 1 in that a method is also recited for the delivery of secure software license information to authorize use of a software product. However, upon invocation of the software product on a computer, in step (c)(ii), the license request is encrypted, rather than signed with the product private key (Specification page 8, lines 6-10, for example); and the license request is decrypted with the product public key in step (d)(i), and encrypted with publisher private key in step (d)(iii) (Specification page 9, lines 1-6, for example).

Independent claim 16 is similar to claim 1 in that a method is also recited for the delivery of secure software license information to authorize use of a software product. However, step (a) recites associating with the software product a publisher certificate

and a product certificate (Specification page 12, line 14 through page 14, line 9, for example). Step (c) recites the license request is transmitted in conjunction with a financial transaction (Specification page 14, line 10-22; page 16, lines 1-2, for example). And step (f) recites validating the license using the publisher and certificate authority certificates... whereby the validation using the publisher and certificate authority certificates establish a trusted link back to the certificate authority (Specification page 18 through page 26, line 5, for example).

Independent claim 24 recites a method for generating and validating a software license for a software product published by a software publisher for the purpose of authorizing use of the software product. Step (a) recites receiving, by the software publisher, a publisher certificate digitally signed by a certificate authority, wherein the publisher certificate includes a publisher ID and step (b) recites embedding the publisher ID within the software product to be authorized (Specification page 10, line 14 through page 14, line 9, for example). Step (c) recites in response to receiving a license request to authorize use of the software product, signing by the software publisher the license for the software product using a private key associated with the publisher certificate, wherein the publisher certificate is included as part of the signature, such that the license for the software product can be validated by; validating the publisher certificate using a certificate authority certificate, validating the signature and contents of the license based on the validated publisher certificate, and validating the software publisher who signed the license by comparing the publisher ID in the publisher certificate contained within the license with the publisher ID in the software product (Specification page 22, line 1-21, for example). Step (d) recites using the validated license contents to control the use of the

software product (Specification page 25, lines 14-17, for example).

VI GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1-26 stand rejected under 35 U.S.C. §102(e) as being unpatentable over U.S. Patent No. 6,898,706 (Venkatesan).

VII ARGUMENTS

U.S. Patent No. 6,898,706 (Venkatesan) fails to anticipate claims 1-26.

Anticipation requires that a prior art reference disclose each and every claim element of the claimed invention. It is respectfully submitted that Venkatesan fails to teach, or even suggest, each and every element of independent claims 1, 12, 16, and 24.

The present invention provides a method and system for the delivery of secure software license information to authorize the use of a software product, such as a software program or software resource. By way of context, the system includes a software product executing on a computer, and a key authority and/or license server connected to the computer system over a network. The software product includes an authorizing program that authorizes use of the software product.

In one embodiment, as recited in independent claims 1 and 12, a method is provided for secure delivery of software license information between the software product and the key authority through the use of private/public keys associated the software publisher of the software product, and private/public keys associated with the software product. In a further embodiment, as recited in independent claim 16, software license information is securely delivered through the use of digital certificates, which include private/public keys as well as other information. In this embodiment, a publisher certificate and a product certificate are associated with the software product to be authorized, wherein both the publisher certificate and the product certificate include respective private/public key pairs, and wherein at least one of the product certificate private and public keys is digitally signed by the publisher private key

associated with the publisher certificate. In a further embodiment, the publisher certificate is digitally signed by a certificate authority, as recited in independent claim 24.

When the software product is invoked, the authorizing program generates a license request containing user and product information. In one embodiment, the license request is secured when transmitted to the key authority and/or license server by digitally signing the license request with the product private key associated with the product certificate. The key authority and/or license server validates the requests and then generates a license with license terms using data extracted from the license request, digitally signs the license with the publisher private key associated with the publisher certificate, and transmits and the signed license back to the authorizing program. The authorizing program then validates the signed license using the publisher public key, and uses the license terms to control the use of the software product.

Referring now to independent claims 1 and 12, the method for delivering secure license terms to a software program refers broadly to private and public key pairs, rather than to certificates. According to the preferred embodiment, the product key is associated with the software publisher key so that only that software publisher can allow the software product to be authorized. To accomplish this, at least one of the product keys is digitally signed by the private key of software publisher. Using the public key of the software publisher, the authorization program can verify that the software publisher who signed the product public key associated with a software product is the same software publisher who signed the license in response to license request.

In independent claim 16, Applicants refer to signed certificates, which have associated private keys. The public keys are part of the certificate, and in this case, the product certificate is digitally signed by the publisher private key. This allows the authorization program to verify that the software publisher who signed its product certificate is the same software publisher who signed the license. Independent claim 24 adds the fact that a certificate authority has a certificate (i.e., a private/public key pair), which is used to sign publisher certificate associated with the software publisher. This means that the protected software program can not only verify that it was authorized by the correct publisher, but can also verify that the software publisher is certified by the certificate authority.

In summary, claims 1, 12 and 16 are directed to methods for *securely delivering license information*, including the initial license request, between a software product and a key authority, while claim 24 is directed to a method of validating license information through a chain of certificates associated with the software product.

In contrast, Venkatesan is directed to techniques for controlling access and use of protected objects by client computer using a digital rights management (DRM) system in the client computer that is based primarily on watermarks being embedded throughout the software object. Applicant acknowledges that Venkatesan may teach a software licensing mechanism, the association of a public and private key pair with a software publisher, and a publisher cryptographically signing a license in response to a license the request. However, despite these teachings, Venkatesan still fails to address the security of the license request and resulting license, as claimed in the present invention for least the following reasons.

i) Claims 1-23 are not anticipated by Venkatesan

First, although Venkatesan may teach associating a private and public key pair with a software publisher, Venkatesan fails to teach or suggest a software product that "includes a software program and *an authorization program within* the software product," as recited in step (a) of claims 1, 12, and 16, where "upon invocation of the software product on a computer," the authorization program generates "a license request," as recited in steps (c) and (c)(i) of claims 1 and 12, and step (b) of claim 16.

Venkatesan fails to teach or suggest that the software object, or part thereof, that has been downloaded to a client PC generates a license request. Instead, Venkatesan clearly teaches that "the user" initiates the license request with the publisher through the client PC (e.g., a web browser), rather than an authorization program. Example portions of Venkatesan state:

> After a user has downloaded a watermarked object, then, in order to use that object, the user, through his(her) client PC, electronically transacts, through the Internet, with publisher's web server. In return for payment of a specific licensing fee to the publisher, this web server downloads to the client PC an electronic license... (Col. 6, lines 21-27) and (col. 14, lines 35 and 41).

> Subsequently, the user, through client PC_j, establishes an Internet session with the publisher's web server and as, indicated by block 540, electronically transacts with that server to obtain a license to use the previously downloaded object.... Once the user makes the selection and authorizes electronic payment for the desired rights, the browser, based on embedded code in the web page, transmits, to the publisher's web server, the rights selection, payment authorization and a computer identification (CID) associated with client PC_j.... Once this information is transmitted to the publisher's web server, that server issues, as indicated by block 550 shown in FIG. 5, an electronic license (L_i) and transmits, as symbolized by line 555, that license to the client PC. (Col. 21, line 66 through col. 22, line 20).

Accordingly, because the generation of the license request is manually initiated by the user by interacting with the PC through a Web browser, Venkatesan fails to teach or suggest that the software object or a part thereof generates the license request upon invitation of the software object.

It should be noted that Venkatesan also provides for an enforcer that looks for watermarks in an object whenever the client computer attempts to access a file containing the protected object. It is also believed that the enforcer cannot be considered analogous to the "authorization program" because the enforcer does not generate a license request. In addition, the enforcer is not part of the protected software object. Rather, the enforcer is part of a digital rights management (DRM) system, which in turn is part of the operating system (col. 18. lines 44-45).

Consequently, Venkatesan's fails to teach or suggest a software product that "includes a software program and *an authorization program within* the software product," where "upon invocation of the software product on a computer," the authorization program generates "a license request," as recited in claims 1, 12, and 16.

Second, although Venkatesan may teach the use of a publisher key, Venkatesan also fails to teach or suggest "associating a *product* private key and public key with the software product", as recited in step (b) of claims 1 and 12, and step (a) of claim 16. On page 7 of the Final Office Action, the Examiner cites figure 5, step 550, of Venkatesan for teaching this step, stating "upon payment by user, publisher issues and downloads to user electronic license with usage rights including secret key." However, nothing pertaining to step 550 teaches or suggests associating a product private and public key pair with a software products/object. The Examiner makes reference to a

"secret key", but Venkatesan describes that this secret key, which is included in the license, "is to decrypt the [software] object. This secret key..., is a symmetric encryption key, i.e., the same key used use by the publisher to encrypt the object (col. 22, lines 25-28). Although Venkatesan's secret key is used to encrypt the software object, and presumably considered by the Examiner to be "associated" with the software object, Venkatesan's secret key is "symmetric", i.e., there is only one. Consequently, there can be no pair of product keys, i.e., a product private key and public key. More importantly, it is believed that Venkatesan's secret key is only used to encrypt and decrypt the software object, but not to "digitally sign the license request," as explained further below.

In addition, contrary to the Examiner's assertion during the rejection of claim 3, it is also believed that Venkatesan's product identification (PID) and certified public key also fail to teach or suggest the claimed product key for the following reasons. First, Venkatesan's product identification (PID) is defined as a value (col., line 64), not as a cryptographic key; and unlike the claimed product key, the PID is not used to digitally sign anything, let alone the license request. Second, the certified public key referred to by the Examiner in step 1122 of Venkatesan also fails to teach or suggest the claimed product key because the certified public key is associated with the client PC, not the software object (col. 30, lines 31-34). Although the certified public key is used to encrypt the license after being provided to the publisher by the client PC as part of the license request, this key is public, not private, and is not used to sign or encrypt the license request, as the claimed product key.

Furthermore, because Venkatesan fails to teach associating a product public key and private key with a software product, Venkatesan cannot teach "digitally signing" "at least one of the product private and public keys with the publisher private key", as recited in step (b) of claims 1 and 12.

One of the claimed elements of the present invention is the fact that the license request generated by the authorization program is delivered securely to the key authority (e.g., step (c)(iii)). The security is provided by "digitally signing the license request with the product private key," as recited in step (c) (ii).

Not only does Venkatesan fail to teach or suggest that some part of the software object that has been downloaded to a client PC generates a license request, as described above, Venkatesan also fails to address providing security for the license request. Venkatesan merely describes that "the user" initiates the license request with the publisher through the client PC (e.g., a web browser), and in return receives a license. Not only is Venkatesan's license request not signed by a product private key, but the license request appears not to be signed or encrypted all. Consequently, Venkatesan fails to teach or suggest "digitally signing the license request with the product private key," as recited in step (c) (ii) of claim 1 and step (d) of claim 16, and fails to teach or suggest "encrypting the license request...," as recited in step (c) (ii) of claim 12.

For at least the reasons stated above, Venkatesan fails to teach or suggest each and every claim element of independent claims 1, 12 and 16. Accordingly, claims claims 1, 12 and 16 are allowable over Venkatesan.

ii) Claims 24-26 are not anticipated by Venkatesan

Independent claim 24 recites an embodiment for generating and validating a software license for a software product published by a software publisher for the purpose of authorizing use of the software product. In this embodiment, claim 24 recites that a certificate authority, which has a certificate (i.e., a private/public key pair). The publisher certificate, which contains the publisher public key, is signed by the certificate authority private key. This means that the protected software program can not only verify that it was authorized by the correct publisher, but can also verify that the software publisher is certified by the certificate authority.

Thus, in this embodiment, the present invention provides a chain of certificates to authorize use of a software program through a license. To run, the software product validates the license, which means validating the certificate chain. As recited in step (c), validating the certificate chain means validating the publisher certificate using a certificate authority certificate, validating the signature and contents of the license based on the validated publisher certificate, and validating the software publisher who signed the license by comparing the publisher ID in the publisher certificate contained within the license with the publisher ID in the software product. Thus, the publisher certificate is cryptographically tied to the certificate authority certificate. The elegance of the solution is that it allows the certificate authority to control how publishers publish the software product, allows software publishers to control how their end-users use their protected software products, and prevents one software publisher from authorizing a software product from another software publisher. It is believed that Venkatesan fails to teach or suggest the combination of elements recited in claim 24, particularly steps (c)(i-iii).

In the Response to Arguments section of the Final Office Action, the Examiner took issue with Applicant's statement in the previous Amendment that unlike the present invention, in Venkatesan, there is no chaining of certificates. To rebut this argument, the Examiner cited col. 9, lines 25-56 of Venkatesan. However, col. 9, lines 25-56 of Venkatesan make clear that the digital signatures and establishment of chains of trust relate to "components of the O/S and particularly throughout enforcer 600 and DRM system 456," rather than to between software publishers and a certificate authority, as claimed.

Accordingly, Venkatesan fails to teach each and every element of claim 24. Therefore, it is respectfully submitted that independent claim 24 is allowable over Venkatesan for at least these reasons.

The dependent claims are allowable because depend from allowable base claims. Accordingly, the reasons set forth above, it is respectfully submitted that Venkatesan fails to teach or suggest the recitations of independent claims 16-19.

For the reasons set forth above, it is respectfully submitted that the §102(e) rejection of claims 1-26 based on Venkatesan has been overcome and that claims 1-26 are patentable. Thus, Appellant respectfully requests that the Board reverse the rejection of all the appealed Claims and find each of these Claims allowable.

Note: For convenience of detachment without disturbing the integrity of the remainder of pages of this Appeal Brief, Appellant's "APPENDIX" sections are contained on separate sheets following the signatory portion of this Appeal Brief.

Respectfully submitted,

STRATEGIC PATENT GROUP

September 17, 2007
Date

/Stephen G. Sullivan/
Stephen G. Sullivan
Attorney for Appellant(s)
Reg. No. 38,329
(650) 493-4540

VIII CLAIMS APPENDIX

1 (Previously presented) A method for the delivery of secure software license information to authorize use of a software product, the method comprising the steps of:

(a) associating with a software publisher a private and public key pair, wherein the software publisher provides the software product and includes a software program and an authorization program within the software product;

(b) associating a product private key and public key with the software product, wherein at least one of the product private and public keys is digitally signed by the publisher private key, and including the product private and public keys with the authorization program;

(c) upon invocation of the software product on a computer,

(i) generating by the authorization program a license request containing user and product information,

(ii) digitally signing the license request with the product private key, and

(iii) transferring the signed license request to a key authority,

(d) in response to the key authority receiving the signed license request,

(i) generating a license using data extracted from the license request and license terms,

(ii) signing the license with the publisher private key, and

(iii) transmitting the signed license to the authorizing program; and

(e) validating the signed license using the publisher public key, and using the license terms to control the use of the software product.

2 (Original) The method of claim 1 further including the step of providing the publisher public key as a certificate.

3 (Original)The method of claim 2 further including the step of providing the product public key as a certificate.

4 (Original) The method of claim 1 further including the step of providing the license in a data exchange format.

5 (Original) The method of claim 4 further including the step of using XML as the data exchange format.

6 (Original) The method of claim 1 further including the step of using the license returned from the key authority to deliver additional key information to the computer.

7 (Original) The method of claim 1 wherein step (d) further includes the step validating the license request using digital certificates.

8 (Original) The method of claim 1 wherein step (e) further included the step of validating the license response using digital certificates.

9 (Original)The method of claim 1 wherein step (e) further included the step of validating the license using the product information in the license, including product ID and publisher ID.

10 (Original)The method of claim 9 further including the step of transferring license terms to a separate security device for controlling the use of the software product.

11 (Previously presented) The method of claim 1 wherein step (e) further included the step of preventing use of the software product on a different computer than that used to generate the license request by using a machine fingerprint embedded in the license request.

12 (Previously presented) A method for the delivery of secure software license information to authorize use of a software product, the method comprising the steps of:

(a) associating with a software publisher a private and public key pair, wherein the software publisher provides the software product and includes a software program and an authorization program within the software product;

(b) associating a product private key and public key with the software product, wherein at least one of the product private and public keys is digitally signed by the publisher private key, and including the product private and public keys with the authorization program;

(c) upon invocation of the software product on a computer,

(i) generating by the authorization program a license request containing user and product information,

(ii) encrypting the license request with the product private key, and

(iii) transferring the encrypted license request to a key authority;

(d) in response to the key authority receiving the encrypted license request,

(i) decrypting the license request with the product public key

(ii) generating a license using data extracted from the license request and license terms,

(iii) encrypting the license with the publisher private key, and

(iv) transmitting the encrypted license to the authorizing program; and

(e) decrypting the license using the publisher public key, and using the license terms to control the use of the software product.

13 (Original)The method of claim 12 wherein step (e) further includes the step of verifying the license using the product information, including the product ID and publisher ID.

14 (Original)The method of claim 13 further including the step of transferring the license terms to a separate security device for controlling the use of the software product.

15 (Previously presented) The method of claim 12 wherein step (e) further includes

the step of preventing use of the software product on a different computer than that used to generate the license request by using a machine fingerprint embedded in the license request.

16 (Previously presented) A method for the delivery of secure software license information to authorize use of a software product, the method comprising the steps of:

a. associating with the software product to be authorized an authorization program and a set of certificates, including a publisher certificate and a product certificate, wherein each certificate contains a public key and is associated with a private key of a public/private key pair, wherein the product certificate is signed by the private key associated with the publisher certificate;

b. upon invocation of the software product on a computer, generating by the authorization program a formatted license request containing user and product information, signed using the private key associated with the product certificate;

c. transmitting the license request to a key authority in conjunction with a financial transaction;

d. generating by the key authority a formatted license that includes license terms, and user and product information extracted from the license request, wherein the license is signed with the publisher private key associated with the publisher certificate;

e. transmitting the signed license to the authorizing program; and

f. validating by the authorization program the license using the publisher and certificate authority certificates and the user and product information contained within the license document, whereby the validation using the publisher and certificate authority certificates establish a trusted link back to the certificate authority; and

g. using the license terms to control the use of the software product on the computer.

17 (Original)The method of claim 16 further including the step of formatting the license request and license documents using the proposed signed XML standard definition.

18 (Original)The method of claim 16 further including the step of signing the product certificate using the publisher's private key, and signing the publisher certificate using the certificate authority's private key, thus establishing a trusted link from the product certificate back to the certificate authority.

19 (Original)The method of claim 16 further including the step of signing the license request using the product private key, and including within the license request the product certificate.

20 (Original)The method of claim 16 further including the step of including financial

transaction information within the license request.

21 (Original)The method of claim 20 further including the step of including financial transaction information within the license response.

22 (Original)The method of claim 16 wherein step (g) further includes the step of transferring the license terms to a separate security device for controlling the use of the software product.

23 (Previously presented) The method of claim 16 wherein step (g) further includes the step of preventing use of the software product on a different computer than that used to generate the license request by using a machine fingerprint embedded in the license request.

24 (Previously presented) A method for generating and validating a software license for a software product published by a software publisher for the purpose of authorizing use of the software product, the method comprising the steps of:

a. receiving, by the software publisher, a publisher certificate digitally signed by a certificate authority, wherein the publisher certificate includes a publisher ID;

b. embedding the publisher ID within the software product to be authorized;

c. in response to receiving a license request to authorize use of the software product, signing by the software publisher the license for the software product

using a private key associated with the publisher certificate, wherein the publisher certificate is included as part of the signature, such that the license for the software product can be validated by,

i. validating the publisher certificate using a certificate authority certificate,

ii. validating the signature and contents of the license based on the validated publisher certificate, and

iii. validating the software publisher who signed the license by comparing the publisher ID in the publisher certificate contained within the license with the publisher ID in the software product; and

d. using the validated license contents to control the use of the software product.

25 (Original) The method of claim 24 further including the step of embedding a product ID within the software product and within the software license.

26 (Original) The method of claim 25 further including the step of validating the license by comparing the product ID stored in the license with the product ID stored within the software product.

IX EVIDENCE APPENDIX

(None)

X RELATED PROCEEDINGS APPENDIX

(None)